We claim:

1. A method for preventing denial of service attacks over a data network including a plurality of traffic flows each formed by a plurality of data packets, the method comprising:

scanning the contents of the data packets;

verifying that the data packets conform to a set of predetermined requirements;

checking if the data packet is associated with a validated traffic flow; and

placing the data packet in a higher priority quality of service if the data packet is associated with a validated traffic flow and to a low priority quality of service if it is not associated with a validated traffic flow.

2. The method of Claim 1 wherein verifying includes insuring that the data packets reorder and reassemble according to a defined policy and insuring that the data packets conform to required parameters.

3. The method of Claim 1 further comprising between verifying and checking:

dropping the data packet if it does not conform to the set of predetermined requirements.

4. The method of Claim 3 wherein scanning includes scanning of the data packet's header information and scanning the data packet's payload contents.

5. The method of Claim 1 wherein the predetermined requirements include packet length, non-overlapping offset fields, and adherence to protocol standards.

6. The method of Claim 5 wherein the validated traffic flows are identified by a state associated with each traffic flow.

7. A method of preventing denial of service attacks on a data network which includes a plurality of traffic flows each formed by multiple data packets having header and payload information, the method using a network device comprising a traffic flow scanning engine and a quality of service processor having a low priority queue and higher priority queues, the method comprising:

scanning the header information using the traffic flow scanning engine;

reordering and reassembling the data packets using the traffic flow scanning engine;

flagging data packets that do not reorder or reassemble correctly to be dropped;

scanning the payload contents using the traffic flow scanning engine;

determining whether the data packets conform to a set of predetermined requirements;

flagging data packets that do not conform to be dropped;

checking if the data packets are associated with a validated traffic flow; and

assigning data packets to a higher priority quality of service if the data packet is associated with a validated traffic flow and to a low priority quality of service if the data packet is not associated with a validated traffic flow.

8. The network device of Claim 7 wherein the set of predetermined requirements include packet length, non-overlapping offset fields, and adherence to protocol standards.

9. The method of Claim 7 wherein flagged data packets are dropped by the traffic flow scanning engine.

10. The method of Claim 7 wherein flagged data packets are dropped by the quality of service processor.

11. The method of Claim 7 wherein the validated traffic flows are identified by a state associated with each traffic flow.

12. A network device for preventing denial of service attacks on a data network which includes a plurality of traffic flows each formed by multiple data packets having contents including header information and payload information, the network device comprising:

a traffic flow scanning engine operable to scan the header and payload information of the data packets, to associate each data packet with a particular traffic flow and to determine whether each traffic flow is a validated traffic flow or a non-validated traffic flow, wherein the traffic flow scanning engine is further operable to reorder and reassemble the data packets and to verify that the data packet conforms to predetermined requirements such that the traffic flow scanning engine produces a conclusion associated with each data packet; and

a quality of service processor connected to the traffic flow scanning engine and operable to place the data packets into a quality of service queue from a plurality of quality of service queues based on the conclusion from the traffic flow scanning engine, wherein data packets from non-validated traffic flows are assigned to a low priority queue and data packets from validated traffic flow are assigned to a higher priority queue based on its contents.

13. The network device of Claim 12 wherein the low priority queue is assigned a maximum percentage of network bandwidth.

14. The network device of Claim 12 wherein data packets that do not reorder or reassemble correctly and data packets that do not conform to the predetermined requirements are dropped by the network device.

15. The network apparatus of Claim 12 wherein the traffic flows are identified by a state associated with each traffic flow, the state representing whether the traffic flow is validated or non-validated.

16. The network apparatus of Claim 12 wherein the set of predetermined requirements include packet length, non-overlapping offset fields, and adherence to protocol standards.